

Completing Approaching Standards

How-To-Guide



DSPT

Better security.
Better care.



Introduction

This guide has been designed to help adult social care providers with achieving 'approaching standards' on the [Data Security and Protection Toolkit \(DSPT\)](#). There are also '[Big Picture Guides](#)' for social care providers which include more detail and background on the DSPT.

The DSPT should be completed every year. It is an online self-assessment tool for demonstrating compliance with the ten data security standards for health and social care organisations. The [Data Security Meta Standard](#) provides more information on what the ten data security standards are and why they are important.

The DSPT will help evidence your compliance with data protection legislation (General Data Protection Regulation or GDPR and Data Protection Act 2018) as well as CQC Key Lines of Enquiry (KLOEs).

It is recommended that social care providers complete the DSPT to Standards Met. However, if this is not achievable the first time, you are able to publish at Approaching Standards. To complete Approaching Standards you just need to complete the evidence items marked as 'Mandatory'. You will then be asked to complete an action plan on how you will complete the remaining items over the next year. The action plan is auto-generated.

How to complete your organisation profile

Once you have registered, you will need to sign in to complete your organisation's profile.

1. Go to <https://www.dsptoolkit.nhs.uk/Account/Login>. The first time you sign in, click "*Forgot your Password*". This will allow you to set your Administrator password.
2. Once signed in, you will see the following screen:



Data Security and Protection Toolkit

My account Logout

Care Home Example Site [Change organisation](#) [Organisation search](#) [News](#) [Help](#)

Assessment [Report an Incident](#) [Admin](#)

Organisation Profile

Before starting your assessment we need to ask you some questions.

The answers you give will:

- tailor your assessment to your organisation's sector
- pre-populate elements of your assessment
- help us to produce national reports

[Continue to questions](#)

Click on the “Continue to questions” button to complete your profile.

3. Choose your organisation type. You should select “Social Care”

Which of these categories best describes your organisation?

Choose one from the list below. [Read about sectors \(opens in a new tab\)](#)

<input type="radio"/> Acute	<input type="radio"/> GP
<input type="radio"/> Ambulance Trust	<input type="radio"/> Local Authority
<input type="radio"/> AQP Clinical Services	<input type="radio"/> Mental Health Trust
<input type="radio"/> AQP Non-Clinical Services	<input type="radio"/> NHS Business Partner
<input type="radio"/> Arms Length Body	<input type="radio"/> NHS Digital
<input type="radio"/> CCG	<input type="radio"/> Optician
<input type="radio"/> Charity / Hospice	<input type="radio"/> Pharmacy
<input type="radio"/> Community Services Provider	<input type="radio"/> Prison
<input type="radio"/> Company	<input type="radio"/> Researcher / Department
<input type="radio"/> CSU	<input type="radio"/> Secondary Use Organisation
<input type="radio"/> Dentist (NHS)	<input checked="" type="radio"/> Social Care
<input type="radio"/> Dentist (Private)	<input type="radio"/> University

[Save](#)

4. You will be asked who has the following roles in your organisation:

- Caldicott Guardian
- Senior Information Risk Owner
- Information Governance Lead
- Data Protection Officer.

You **do not** have to enter any details. If you click the “*continue*” button you will move on to the next page.

None of these roles are well-known in adult social care. There is more detail about each role in our guidance on [Data Security and Protection Responsibilities](#).

5. You will be asked if your organisation uses NHSmail or has a Cyber Essentials Plus certification. Make sure you select the right option or “Not Sure” if you are uncertain.
6. Check your answers and make changes if necessary. Once you’re happy, click “*Accept and Submit*”. You can go back and make changes at any point.

How to set up other users

You can share your work on the DSPT with several people. As an administrator, you can add more users and assign their access level.

1. Sign in to the DSPT and click on “*Admin*” in the dark bar running across towards the top of the screen. This will reveal a drop-down list:

Manage users
Organisation details
Organisation profile

Select “*Manage users*”.

2. On the Manage users page, you can add more users. Users can be allocated one of three roles:
 - a. Auditor - view assertions/evidence/organisation profile, reset own password and update own personal details.
 - b. Member - view assertions, view/add/edit evidence, view organisation profile (but not edit), reset own password and update own personal details.
 - c. Administrator member - view and confirm assertions, view/add/edit evidence, allocate assertion owners, submit and publish assessment, view and edit organisation profile, create and edit users for own organisation, reset own password and update own personal details.

Completing your Assessment

INTRODUCTION

Once you have completed your profile questions, the Social Care Assessment is displayed:

Social Care Assessment

Key data security requirements for social care organisations are listed below. Please respond to the following requirements and publish your assessment.

Important
If you only respond to the MANDATORY requirements, you will be asked to provide an action plan which identifies the steps your organisation will take to meet the full standard

Staffing and roles

1.1.2	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory
2.2.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory
2.2.2	Do all employment contracts, and volunteer agreements, contain data security requirements?	Mandatory
3.1.1	Has a training needs analysis covering data security and protection, and cyber security, been completed since 1st April 2020?	
3.2.1	Have at least 95% of staff, directors, trustees and volunteers in your organisation completed training on data security and protection, and cyber security, since 1st April 2020?	
3.4.1	Have the people with responsibility for data security and protection received training suitable for their role?	
4.1.1	Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?	Mandatory

Policies and procedures

1.2.1	Does your organisation have up to date policies in place for data protection and for data and cyber security?	Mandatory
-------	---------------------------------------------------------------------------------------------------------------	-----------

Evidence items are numbered and organised under four headings:

- Staffing and roles
- Policies and procedures
- Data security
- IT systems and devices

To achieve ‘Approaching Standards’, you must complete all evidence items shown as MANDATORY. If you complete all of the evidence items then you can achieve ‘Standards Met’, we have a separate guide on [completing standards met](#).

There is no specific order to completing the DSPT. You can start anywhere and move back and forth between the evidence items. The system will autosave at regular intervals.

HOW TO COMPLETE AN EVIDENCE ITEM

To complete an evidence item, click on it. This opens a dialogue box to complete.

Evidence item 1.1.2

Who has responsibility for data security and protection and how has this responsibility been formally assigned?

Whilst data security and protection is everybody's business, someone within your organisation must take overall senior responsibility for it. There must be at least one named person who leads on data security and protection. Their responsibility is to provide leadership and guidance from a senior level.

In the text box, write the name(s) of the person or people within your organisation with overall responsibility for data security and protection. Then, for each person, describe how this responsibility has been formally assigned to them. For instance, this responsibility could form part of their job description, or be noted in the minutes of a management meeting, or be in an email from the appropriate director in your organisation. Your organisation may also have additional specialised roles, for example a Data Protection Officer (DPO).

[Read more about data security and protection responsibilities and specialised roles.](#)

Comments (optional)

Save or Cancel

In this example, type text into this box.

Once you have filled in the box, click "Save". This will close the box, and the evidence item will be marked as "COMPLETED".

Staffing and roles		
1.1.2	Who has responsibility for data security and protection and how has this responsibility been formally assigned?	Mandatory COMPLETED
2.2.1	Does your organisation have an induction process that covers data security and protection, and cyber security?	Mandatory
2.2.2	Do all employment contracts, and volunteer agreements, contain data security requirements?	Mandatory

The following sections describe all the mandatory evidence items in detail, with advice on how to complete them, plus links to a range of relevant resources.

Staffing and Roles

1.1.5 Who has responsibility for data security and protection and how has this responsibility been formally assigned?

Tool Tip	<p>Whilst data security and data protection is everybody's business, there must be a named person within your organisation who takes overall senior responsibility for data security and protection issues. Their responsibility is to provide senior level leadership and guidance.</p> <p>In the text box, name the person or people within your organisation with overall responsibility for data security and protection, along with their roles. Then, for each person, describe how this responsibility has been formally assigned to them. For instance, this responsibility could form part of their job description, or be noted in the minutes of a management meeting, or be in an email from the appropriate director in your organisation. Your organisation may also have additional specialised roles, for example a Data Protection Officer or a Caldicott Guardian.</p> <p>You can read more about data security and protection responsibilities and specialised roles on the Digital Social Care Website.</p>
Video Guide	https://vimeo.com/654218225

2.1.1 Does your organisation have an induction process that covers data security and protection, and cyber security?

Tool Tip	<p>All new staff, directors, trustees and volunteers who have access to personal data, should have an induction that covers data security and protection as well as cyber security. It is good practice to keep records of who has been inducted and to review the induction process on a regular basis to ensure it is effective and up to date.</p> <p>There is 'staff guidance for data sharing' available: https://www.digitalsocialcare.co.uk/latestguidance/staff-guidance/ </p>
Video Guide	https://vimeo.com/654230540

2.1.2 Do all employment contracts, and volunteer agreements, contain data security requirements?

Tool Tip	<p>Clauses in contracts or agreements should reference data security (confidentiality, integrity and availability). Many contracts commonly focus on just confidentiality.</p> <p>Your organisation's staff employment contracts, and volunteer and trustee agreements if you have them, should be reviewed to see if they need to be updated to include a clause on data security.</p> <p>There is an example staff contract clause available: https://www.digitalsocialcare.co.uk/latest-guidance/staff-guidance/ </p>
Video Guide	<p>https://vimeo.com/654230540</p>

4.1.1 Does your organisation have an up to date record of staff, and volunteers if you have them, and their roles?

Tool Tip	<p>Your organisation must have a list of all staff, and volunteers if you have them, and their current role. This list should be kept up to date, including any change of role, new starters and removal of leavers.</p> <p>This might be linked to your existing payroll or rostering system.</p>
Video Guide	<p>https://vimeo.com/542130079</p>

Policies and Procedures

1.1.1 What is your organisation's Information Commissioner's Office (ICO) registration number?

Tool Tip Registration with the ICO is a legal requirement for every organisation that processes personal information, unless they are exempt as a small charity. If your organisation is not already registered, you should [register as a matter of urgency](#).

You can check whether you are registered and what your ICO registration number is on the [Information Commissioner's Office website](#).

Video Guide <https://vimeo.com/654218225>

1.1.2 Does your organisation have an up to date list of the ways in which it holds and shares different types of personal and sensitive information?

Tool Tip To be compliant with data protection legislation you must keep a register of all of the information your organisation stores, shares and receives. The exact information you should include is explained in detail in the guidance below.

This list is called an Information Asset Register (IAR) and it should detail where and how the information is held and how you keep it safe. You should also have a list or lists of the types of personal data that are shared with others, for example needs assessments, prescriptions, payslips, care plans. This list is called a Record of Processing Activities (ROPA) and should detail how the data is shared and how your organisation keeps it safe. You can combine these into one document, but it is fine to have two separate documents.

The register should have been reviewed and approved by the management team at least once in the last twelve months.

Example IARs and ROPAs are available:

<https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/>

Video Guide <https://vimeo.com/654218225>

1.1.3 Does your organisation have a privacy notice(s)?

Tool Tip	<p>If you use and share personal data then you must tell people what you are doing with it. This includes why you need the data, what you'll do with it, who you're going to share it with and individual's rights under data protection legislation for example, the right to access their information.</p> <p>This should be set out in writing in 'a privacy notice'. You should provide this information in a clear, open and honest way using language which is easy to read and understand. Your privacy notice should cover all data you process for example the data relating to the people you support and their relatives, staff, volunteers, members of the public. You may have more than one privacy notice e.g. one for staff and another one for the people you support.</p> <p>An example privacy notice is available: https://www.digitalsocialcare.co.uk/latest-guidance/how-to-document-your-data-processing/</p>
Video Guide	https://vimeo.com/654220870

1.3.1 Does your organisation have up to date policies in place for data protection and for data and cyber security?

Tool Tip	<p>You should have policies and staff guidance in place communicating your organisation's principles and procedures for data protection.</p> <ul style="list-style-type: none"> • data protection • data quality • record keeping • data security • where relevant, network security <p>These should be updated every three years at the minimum, and locally maintain evidence of when each update was made.</p> <p>Policy templates are available: https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/.</p>
Video Guide	https://vimeo.com/654222813

1.3.7 Does your organisation's data protection policy describe how you keep personal data safe and secure?

Tool Tip	<p>Your policy should describe how your organisation identifies and accounts for privacy and data protection issues before commencing a new project or process. This is called 'data protection by design'. This might be a new data sharing initiative, for example, becoming part of a shared care record, setting up a new care record system, or using personal data for a new purpose such as research.</p> <p>Your policy should also explain how your organisation only collects, uses and shares the minimum amount of data necessary for the purpose; how you ensure that data is only available to those who need it; how you store data only for as long as is needed; and how you let people know what you are doing with their data. This is called 'data protection by default'.</p> <p>There is guidance on data protection by design and by default on the ICO's website. Our Data Protection Policy template covers this subject: https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/.</p>
Video Guide	https://vimeo.com/654222813

1.3.8 Does your organisation's data protection policy describe how you identify and minimise risks to personal data when introducing, or changing, a process or starting a new project involving personal data?

Tool Tip	<p>Your policy should describe the process that your organisation has in place to make sure that it systematically identifies and minimises the data protection risks of any new project or plan that involves processing personal data. For example, when you introduce a new care recording system; if you install CCTV; if you use new remote care or monitoring technology; if you share data for research or marketing purposes.</p> <p>This type of risk assessment is called a Data Protection Impact Assessment (DPIA). Your organisation should consider whether it needs to carry out a DPIA at the early stages of any new project if it plans to process personal data. A DPIA should follow relevant guidance from the Information Commissioner's Office (ICO).</p>
Video Guide	https://vimeo.com/654222813

1.4.1 Does your organisation have a timetable which sets out how long you retain records for?

Tool Tip	<p>Your organisation should have in place and follow a retention timetable for all the different types of records that it holds, including finance, staffing and care records.</p> <p>The timetable, or schedule as it sometimes called, should be based on the Records Management Code of Practice 2021.</p>
Video Guide	<p>https://vimeo.com/654227822</p>

1.4.2 If your organisation uses third parties to destroy records or equipment that hold personal data, is there a written contract in place that has been reviewed in the last twelve months? This contract should meet the requirements set out in data protection regulations.

Tool Tip	<p>It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old computers and laptops, mobile phones, CDs and memory sticks.</p> <p>If your organisation uses a contractor to destroy any records or equipment, such as a document shredding company or IT recycling organisation, then the contract(s) or other written confirmation with third parties must include the requirement to have appropriate security measures and the facility to allow audit by your organisation. Further information about the destruction of records is in chapter 5 of the Records Management Code of Practice.</p> <p>If you do not use third parties to destroy records or equipment, then tick and write “Not applicable” in the comments box. Advice on contracts for secure disposal of personal data is available: https://www.digitalsocialcare.co.uk/latestguidance/contract-guidance/</p>
Video Guide	<p>https://vimeo.com/654227822</p>

1.4.3 If your organisation destroys any records or equipment that hold personal data, how does it make sure that this is done securely?

Tool Tip	<p>It is important that when there is no longer a valid reason to keep personal data that it is disposed of securely. This applies to paper documents, electronic records and equipment, such as old compute and laptops, mobile phones, CDs and memory sticks. If anyone in your organisation destroys any records or equipment themselves, such as shredding documents, briefly describe how the organisation makes sure that this is done securely. If you do not destroy records or equipment yourselves, or only use a third party to do so, write “Not applicable” in the text box.</p> <p>We have a Record Keeping policy that has details on the safe destruction of personal data: https://www.digitalsocialcare.co.uk//latest-guidance/template-policies/</p>
Video Guide	<p>https://vimeo.com/654227822</p>

10.1.2 Does your organisation have a list of its suppliers that handle personal information, the products and services they deliver, and their contact details?

Tool Tip	<p>Your organisation should have a list or lists of the external suppliers that handle personal information such as IT or care planning systems suppliers, IT support, accountancy, DBS checks, HR and payroll services, showing the system or services provided.</p> <p>If you have no such suppliers, then tick and write “Not applicable” in the comments box.</p> <p>A template example is available from https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/manage-your-suppliers/</p>
Video Guide	<p>https://vimeo.com/542131869</p>

Data Security

1.3.12 How does your organisation make sure that paper records are safe when taken out of the building?

Tool Tip Paper records may be taken out of your organisation’s building(s), for example for hospital appointments or visits to people’s homes. Leaving documents in cars, for instance, can be risky. How does your organisation make sure paper records are kept safe when ‘on the move’?

If you do not have any paper records or do not take them off site, write “Not applicable” in the text box.

Video Guide <https://vimeo.com/654222813>

1.3.13 Briefly describe the physical controls your buildings have that prevent unauthorised access to personal data.

Tool Tip Physical controls that support data protection include lockable doors, windows and cupboards, clear desk procedure, security badges, key coded locks to access secure areas etc.

Provide details at high level and, if you have more than one building, summarise how compliance is assured across your organisation’s sites.

Video Guide <https://vimeo.com/654222813>

6.1.1 Does your organisation have a system in place to report data breaches?

Tool Tip All staff, and volunteers if you have them, are responsible for noticing and reporting data breaches and it is vital that you have a robust reporting system in your organisation. There is an incident reporting tool within this toolkit which should be used to report health and care incidents to Information Commissioner’s Office ICO.

If you are not sure whether or not to inform the Information Commissioner’s Office of a breach, the toolkit’s incident reporting tool and guide can help you to decide.

Video Guide	https://vimeo.com/542131181
--------------------	-----------------------------------------------------------------------

6.1.2 If your organisation has had a data breach, were the management team notified, and did they approve the actions planned to minimise the risk of a recurrence?

Tool Tip In the event of a data breach the management team of your organisation, or nominated person, should be notified of the breach and any associated action plans or lessons learnt.

If no breaches in the last 12 months then please tick and write "Not applicable" in the comments box.

Video Guide	https://vimeo.com/542131181
--------------------	-----------------------------------------------------------------------

6.1.3 If your organisation has had a data breach, were all individuals who were affected informed?

Tool Tip If your organisation has had a data breach that is likely to result in a high risk of adversely affecting individuals' rights and freedoms - e.g. damage to reputation, financial loss, unfair discrimination, or other significant loss - you must inform the individual(s) affected as soon as possible.

If your organisation has had no such breaches in the last 12 months then please tick and write "Not applicable" in the comments box.

More information is available from the Information Commissioner's Office:
<https://ico.org.uk/for-organisations/guide-to-the-general-dataprotection-regulation-gdpr/personal-data-breaches/>

Video Guide	https://vimeo.com/542131181
--------------------	-----------------------------------------------------------------------

IT Systems and Devices

1.3.11 If staff, directors, trustees and volunteers use their own devices (e.g. phones) for work purposes, does your organisation have a bring your own device policy and is there evidence of how this policy is enforced?

Tool Tip The devices referred in this question include laptops, tablets, mobile phones, CDs, USB sticks etc. This applies to use of devices whether the person is on duty or not e.g. if they access your system(s) when not on shift. Please upload your Bring Your Own Device policy and any associated guidance, and evidence of how this policy is enforced.

If nobody uses their own devices, then tick and write “Not applicable” in the comments box.

A template Bring Your Own Device (BYOD) policy, and examples of how this policy might be enforced, is available:

<https://www.digitalsocialcare.co.uk/latest-guidance/template-policies/>

Video Guide <https://vimeo.com/654222813>

4.2.4 Does your organisation have a reliable way of removing or amending people’s access to IT systems when they leave or change roles?

Tool Tip When people change roles or leave your organisation, there needs to be a reliable way to amend or remove their access to your IT system(s). This could be by periodic audit to make sure that people’s access rights are at the right level. It is important that leavers who had access to personal data have their access rights revoked in line with your policies and procedures. This includes access to shared email addresses.

If your organisation does not use any IT systems, then tick and write “Not applicable” in the comments box

Video Guide <https://vimeo.com/542130481>

4.5.4 How does your organisation make sure that staff, directors, trustees and volunteers use good password practice?

Tool Tip	<p>If your organisation has any IT systems or computers, it should provide advice for setting and managing passwords. Each person should have their own password to access the computer, laptop or tablet that they are using and a separate password for other systems. These passwords should be 'strong' i.e. hard to guess.</p> <p>This could be enforced through technical controls i.e. your system(s) require a minimum number of characters or a mixture of letters and numbers in a password.</p> <p>If your organisation does not use any IT systems, computers or other devices, write "Not applicable" in the text box.</p> <p>Information about good password practice is available: https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/use-strong-passwords/</p>
-----------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Video Guide	
--------------------	--

6.2.1 Do all the computers and other devices used across your organisation have antivirus/antimalware software which is kept up to date?

Tool Tip	<p>This applies to all servers, desktop computers, laptop computers, and tablets. Note that antivirus software and antimalware software are the same thing – they both perform the same functions. You may need to ask your IT supplier to assist with answering this question.</p> <p>If your organisation does not use any computers or other devices, then tick and write "Not applicable" in the comments box.</p> <p>Further information is available: https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/have-up-to-date-antivirus-software/</p>
-----------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Video Guide	https://vimeo.com/digitalsocialcare/62
--------------------	---------------------------------------------------------------------------------------------

7.3.1 How does your organisation make sure that there are working backups of all important data and information?

Tool Tip	<p>It is important to make sure that backups are being done regularly, that they are successful and that they include the right files and systems. Briefly explain how your organisation’s back up systems work and how you have tested them.</p> <p>You may need to ask your IT supplier to assist with answering this question. If your organisation does not use any computers or IT systems, write “Not applicable” in the text box.</p> <p>For advice about backups, see https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/back-up-your-data/</p>
Video Guide	https://vimeo.com/654232639

7.3.2 All emergency contacts are kept securely, in hardcopy and are up-to-date.

Tool Tip	<p>Contacts include phone number as well as email.</p>
Video Guide	https://vimeo.com/654232639

8.3.5 How does your organisation make sure that the latest software updates are downloaded and installed?

Tool Tip	<p>It is important that your organisation’s IT system(s) and devices have the latest software and application updates installed. Most software can be set to apply automatic updates when they become available from the manufacturer. You may need to ask your IT supplier to assist with answering this question.</p> <p>If your organisation does not use any IT systems, devices or software, write “Not applicable” in the text box.</p> <p>Further information is available from https://www.digitalsocialcare.co.uk/data-security-protecting-my-information/cyber-security/install-the-latest-software-updates/</p>
Video Guide	https://vimeo.com/542131689

How to publish at Approaching Standards

When you have completed all items marked as mandatory you can publish at Approaching Standards level. Click on this blue button at the bottom of the page:

Publish Approaching Standards Assessment

You will then see the following screen:

[← Assessment](#)

Provide an action plan

Thank you for responding to all the mandatory requirements


- You should now download a [blank action plan template](#), which lists the requirements you have not yet responded to.
- You should then complete this plan and upload a copy here, as proof you are approaching the Data Security and Protection Toolkit standard.
- You will then be able to publish your 'Approaching Standards' assessment.

Upload file

Click here to download a blank action plan template and complete this for the requirements you haven't completed yet.

When you have completed your action plan, upload it here:

Upload file

Drag and drop Action Plan or [click to browse](#) 

Publish Approaching Standards Assessment

You will be able to see the file you have uploaded. If you need to make any changes you can remove and replace the file.

Upload file

Document Currently Saved:

DSPT_Action_plan_RCN01_04032021_2121.xl SX	Remove	Replace
-----------------------------------------------	--------	---------

Publish Approaching Standards Assessment

Once this is done, click “Publish Approaching Standards Assessment”.

You will then be asked to confirm that your organisation profile is correct. Make any changes you need and then click “Publish Approaching Standards Assessment”.

Publish Approaching Standards Assessment

By clicking 'Publish Approaching Standards Assessment' you are confirming that your organisation has started to implement key data security measures and that you will deliver the required actions to meet the full standard.

Confirmation of the publication will be sent to you at

Publish Approaching Standards Assessment

When you have done this, you will receive an email confirming that you have published and confirmation will appear on the screen.

Your assessment has been published

Confirmation of your publication has been emailed to you. If you do not receive the email confirmation, please check your spam or junk email folder.

Remember that if you make changes to your assessment you will need to publish your assessment again.

[View All Publications](#)

Congratulations, you have completed approaching standards on the DSPT.

If you want to move onto standards met, we have [guidance available](#).

Multisite Assessments

If you are publishing as a head office on behalf of your sites, you will see an

Help!

If you are having technical difficulties with any part of the DSPT, please [contact the DSPT team](#).

If you have any concerns or questions on any of the materials mentioned in this guide, please contact us: help@digitalsocialcare.co.uk